

Congressman Tom Udall (NM-3)
House Veterans Affairs Committee
Oversight Hearing on the VA Data Theft of veterans' personal information
May 25, 2006

Mr. Chairman,

“Deter identity thieves by safeguarding your information.” This is the very first commandment of protecting one’s identity. Yet, we are here today to accept testimony of how the United States Department of Veterans Affairs found themselves investigating the theft of the personal information for 26.5 million American veterans. Mr. Secretary, this is irresponsibility of the highest order.

The fact that one individual, in this case a VA data analyst, has the ability to walk off of VA premises with personal information on 26.5 million veterans is in and of itself a matter that must be immediately addressed. There is no doubt that VA employees are hard-working individuals who may find themselves taking resources off VA premises for work purposes. But to allow the opportunity for such sensitive information, and in such a massive amount, to be transported is an absolute error. Unfortunately, this is only the beginning of the problems catalyzed by the VA’s announcement on Monday.

During a briefing earlier this week, representatives from the VA were unable to answer what I believe are basic questions: What information was taken by the data analyst? For what purposes was this data taken? Was the data encrypted? Were health, disability ratings, or financial codes included in the data? Why was the analyst able to take the information out of a secure area and keep it at home? Do other employees have similar data at home, either with or without the permission of their superiors? Has this policy been changed, or has it at least been suspended pending this investigation? The VA was unable to provide answers to any of these questions.

These legitimate and necessary questions are ones that should be, and are being, asked by law enforcement officials. But now, we have learned, the VA knew of the data theft for two weeks before alerting authorities, and nineteen days before making it public. During this time, the VA considered the loss of sensitive information on every American veteran simply an “internal issue.” If this is the VA’s perspective on protecting veterans’ information, it has lost its focus on the mission to “serve those who have served.”

Again, there are obvious reasons why some questions cannot yet be publicly answered, as the FBI, VA IG and local authorities continues to investigate the theft. However, I pose all of these questions again today in hopes that those which can be answered will be answered. This is more than simply a question of security threats or personnel policy. This issue transcends bureaucratic process because it has directly and completely placed the personal, private information of every veteran in America in jeopardy.

Every member of this committee represents thousands of veterans who are now worriedly watching their credit reports, their credit card statements and their bank records, fearing that they will become a victim of identity theft. That some of them have taken every precaution to safeguard against this situation yet still find their information vulnerable is wrong. Mr. Secretary, I would offer the strongest urging that you undertake a serious reevaluation of VA policy on these matters and that you ensure new regulations and rules within the Department that will better secure veterans' information are put into place as soon as is possible. As always, this committee stands ready to assist the Secretary with this and all veterans' issues, and I greatly hope that in the very near future we will be hearing good news on why our veterans no longer need worry that their personal information will not fall into the wrong hands.

Thank you, Mr. Chairman.